



Enero 2014

Versión 1.1.

Manual del servicio de certificación con clave pública para el acceso a TARGET2 a través de internet.

Manual de certificación con clave pública

ÍNDICE

1 Información general

Este Manual establece los procedimientos seguidos por Banca de Italia como Autoridad de Certificación acreditada para la emisión y utilización de certificados electrónicos para el acceso a TARGET2 a través de Internet.

El Servicio lo proporciona Banca de Italia en nombre del Eurosistema.

Este Manual se dirige a:

- Los bancos centrales participantes en TARGET2;
- Las entidades de crédito y otras entidades autorizadas a participar en TARGET2 accediendo a través de Internet;
- Los titulares de los certificados autorizados por los participantes.

2 Datos de identificación

2.1 La Autoridad de Certificación

Nombre	Banca d'Italia
	Via Nazionale, 91 – 00184 ROMA
Representante legal	Gobernador
Sitio web	www.bancaditalia.it

2.2 El manual del usuario

Este Manual para el servicio de certificación con clave pública proporcionado por Banca de Italia, está disponible en el apartado para bancos de la web del TARGET2-ECB (https://target2.ecb.int)[1]

3 Obligaciones de la Autoridad de Certificación, de los Bancos Centrales Nacionales, de los participantes y de los titulares de los certificados

3.1 Obligaciones de la Autoridad de Certificación

La Autoridad de Certificación deberá:

1 Adoptar las medidas organizativas y técnicas para evitar daños a terceras partes.

[1] http://www.ecb.europa.eu/pub/pdf/other/target2progressreport5-a1-informationguidetarget2usersen.pdf

2 Proporcionar información clara y completa sobre el procedimiento de certificación, los requisitos técnicos para acceder y las restricciones de uso.
3 Proporcionar un servicio rápido y seguro para la emisión, suspensión y reactivación de los certificados así como para la revocación y renovación de los mismos y asegurar el funcionamiento eficiente, oportuno y seguro de las listas de certificados emitidos, suspendidos y revocados.
4 Asegurar que se fija de forma precisa la fecha y hora de emisión, revocación y suspensión de los certificados electrónicos.
5 No copiar ni conservar las claves privadas de los titulares de los certificados.
6 Preparar toda la información necesaria, en particular, los términos y condiciones exactos que regulan el uso de los certificados, incluyendo sus restricciones. Deberá hacer pública dicha información a las partes interesadas en el servicio de certificación.
7 Usar sistemas fiables para la gestión del registro de certificados, con procedimientos que aseguren que sólo personas autorizadas realizarán las altas y modificaciones, que puede ser comprobada la autenticidad de los datos y que las personas autorizadas advertirán cualquier circunstancia que ponga en peligro la seguridad.
8 En el caso de cese de su actividad, notificar a los titulares con al menos sesenta días de antelación que los certificados que no hayan expirado, serán revocados y efectivamente los revocará a su debido tiempo.
9 Adoptar medidas de seguridad para el tratamiento de la información de carácter personal de acuerdo con la legislación italiana vigente.

La Autoridad de Certificación es responsable del cumplimiento de todas las obligaciones legales contenidas en este Manual.

La Autoridad de Certificación no será responsable de:

1 Las consecuencias derivadas de errores de los titulares de los certificados en el cumplimiento de las normas de los procedimientos operativos y métodos especificados en este Manual.
2 Fallos en el cumplimiento de sus obligaciones, provocados por causas ajenas a su voluntad.

3.2 Obligaciones de los Bancos Centrales Nacionales

Los bancos centrales deberán:

1 Facilitar toda la información relevante proporcionada por la Autoridad de Certificación a los participantes y titulares de los certificados.
2 Garantizar la identidad de la persona que solicita la certificación.
3 Verificar la autenticidad de la solicitud.

4 Hacer llegar puntualmente a la Autoridad de Certificación todos los formularios y cualquier comunicación recibida de los participantes siguiendo los procedimientos establecidos en este Manual.

5 Hacer llegar puntualmente a los participantes todos los formularios y cualquier otra comunicación recibida de la Autoridad de Certificación siguiendo los procedimientos establecidos en este Manual.

3.3 Obligaciones de los participantes

Los participantes deberán:

1 Solicitar la emisión de los certificados, siguiendo los procedimientos especificados en este Manual.

2 Solicitar la suspensión y la reactivación así como la revocación y la renovación de los certificados de acuerdo con los procedimientos especificados en este Manual siempre que la base sobre la que se emitió el certificado al titular varíe o deje de existir o en caso de que cese la actividad propia (por motivo de fusión, liquidación, etc.).

3 Adoptar las medidas organizativas y de precaución que sirvan para asegurar la utilización de los certificados de conformidad con las reglas establecidas en este Manual.

4 Notificar puntualmente a la Autoridad de Certificación, a través de su banco central nacional responsable, los cambios en la información indicada en los formularios en el momento de la emisión de los certificados y que sea relevante para su utilización.

5 Asegurar que los titulares de los certificados conocen y cumplen con sus obligaciones.

3.4 Obligaciones de los titulares de los certificados

Es obligación de los titulares de los certificados mantener en lugar seguro los dispositivos de seguridad y adoptar las medidas técnicas y organizativas para evitar cualquier perjuicio a terceras partes y asegurar el uso personal de estos dispositivos.

Los titulares de los certificados deben también:

6 Proporcionar toda la información solicitada por el banco central responsable, garantizando su exactitud bajo su propia responsabilidad.

7 Notificar a la Autoridad de Certificación, a través de su banco central responsable, cualquier modificación en la información proporcionada en el momento del registro: datos personales, residencia, números de teléfono, direcciones de correo electrónico, etc.

8 Conservar los dispositivos que contienen los certificados con la máxima diligencia y separados de los códigos secretos (PIN y PUK), para asegurar su integridad y máxima confidencialidad.

9 No utilizar los certificados para otros fines diferentes a aquellos para los que se emitieron.

10 Trasmitir la información necesaria y solicitar la suspensión y reactivación así como la revocación y renovación del certificado siguiendo los procedimientos definidos en este Manual.
11 Solicitar la suspensión inmediata de los certificados cuando los dispositivos que contienen las claves sean defectuosos o ya no estén en posesión de su titular.
12 Notificar al banco central responsable la pérdida o robo del dispositivo de seguridad.

4 Procedimiento para el registro e identificación de usuarios

Esta sección describe el procedimiento para la emisión inicial de certificados, que incluye la identificación del solicitante y su registro.

4.1 Formulario de solicitud

Las personas que soliciten la emisión de certificados deben estar identificadas y designadas por la entidad de crédito en cuyo nombre operarán de conformidad con su relación laboral o profesional; el banco central nacional responsable garantiza la correcta identificación del solicitante de acuerdo con las reglas establecidas a nivel nacional con los participantes.
El participante da fe de que entiende el contenido de este Manual y se compromete a cumplir con sus obligaciones.
La persona designada (titular del certificado) completa y firma la solicitud, que:

1 indicará la información que identifica al solicitante (titular del certificado), incluyendo un número único de identificación (por ej., número de identificación fiscal, D.N.I., etc)
2 contendrá una declaración en la que el solicitante (titular del certificado) da fe de que la información proporcionada es exacta y se compromete a notificar cualquier cambio en ella;
3 contendrá una declaración en la que el solicitante (titular del certificado) da fe de que ha recibido nota informativa sobre protección de datos de carácter personal;
4 deberá ir acompañada de una copia del documento de identificación del solicitante (titular del certificado)
5 será refrendado por una persona autorizada por el participante.

Esta documentación será remitida al banco central nacional responsable del participante.

4.2 Registro de usuarios

Después de realizar las comprobaciones que sean de su competencia, el banco central nacional responsable hará seguir la solicitud de certificados a la “SSP Service Desk”,

quien introducirá todos los datos necesarios para la emisión de los certificados en el archivo de registro.
Cuando no se acepte un formulario, la “SSP Service Desk” informará al banco central correspondiente que informará a su vez al participante.

4.3 Entrega de los dispositivos de seguridad

El banco central responsable, después de recibir los sobres que contienen, respectivamente, la tarjeta (*token USB*) y los códigos secretos (PIN y PUK)[2] los enviará al participante que lo haya solicitado para que los entregue al titular del certificado; el banco central nacional pondrá a disposición del solicitante (titular del certificado) una versión electrónica de este Manual.
Los participantes crearán un registro para la entrega que recogerá las firmas de la persona responsable de la entrega y la del titular del certificado.
Los participantes informarán al banco central responsable que el certificado ha sido entregado a su titular y el banco central notificará la entrega a la “SSP Service Desk” para activar el certificado.

5 Procedimiento de emisión de certificados

Un certificado asocia la clave pública de una par de claves asimétricas a un conjunto de datos que identifican a una persona (el titular del certificado) que posee la correspondiente clave privada.
Esa asociación queda garantizada con la incorporación al certificado de la firma de la Autoridad de Certificación realizada con su clave privada de certificación.

5.1 Información que contiene un certificado

Un certificado contiene:

1 Un número de serie u otro código de identificación del certificado.
2 Nombre de la Autoridad de Certificación y país en el que está establecida.
3 Código de identificación del titular del certificado en la Autoridad de Certificación.
4 Nombre, Apellido, número único de identificación y fecha de nacimiento del titular del certificado.
5 Período de validez del certificado.
6 Firma digital de la Autoridad de Certificación.

---

[2] El PIN debe introducirse para firmar y realizar otras operaciones relacionadas con el uso de los certificados y debe ser cambiado por el titular la primera vez que lo utilice.
El PUK sirve para desbloquear la tarjeta después de introducir un PIN incorrecto un determinado número de veces.

7 Número de la clave pública.
8 Algoritmos de generación y verificación.
9 Algoritmo de firma del certificado.
10 Tipo de par de claves según el uso asignado al certificado.

Para identificar al titular se seguirán las normas del Distinguished Name (DN) contenidas en la ISO 9594-1 (1997)
La información personal contenida en el certificado debe utilizarse sólo para identificar al titular en relación a las operaciones a las que esté autorizado a llevar a cabo.

La Entidad de Certificación conservará la información relacionada al certificado por un período no inferior a veinte años desde su fecha de revocación o expiración.

5.2 Períodos de validez de las claves y los certificados

Los certificados de firma emitidos a los titulares son válidos hasta los 3 años desde su emisión.

6 Procedimiento de emisión de certificados

La Autoridad de Certificación suspende o revoca los certificados incorporando su número de serie en las listas de certificados suspendidos o revocados.[3]
La suspensión o revocación de un certificado tiene efecto desde el momento de la incorporación del certificado en las mencionadas listas.

Cuando un certificado se suspende, su validez se interrumpe temporalmente.
Cuando un certificado se revoca deja de tener validez.

6.1 Suspensión o revocación de certificados

El titular del certificado o el participante puede solicitar que la validez de un certificado sea suspendida o el certificado sea revocado por alguna de las razones recogidas en el punto 6.2.

Cuando la Autoridad de Certificación tenga conocimiento de un posible mal uso, falsificación o negligencia, puede suspender el certificado después de notificarlo a su titular a través de la "SSP Service Desk" y al banco central responsable. En caso de emergencia, el certificado podrá ser suspendido antes de que el titular sea notificado.

En el caso de:

- pérdida,

[3] Las dos listas se presentan actualmente para consulta como una única lista que incluye tanto los certificados suspendidos como los revocados, distinguiendo las distintas "causas".

- robo, o
- pérdida de seguridad de la tarjeta o del *token USB,*

El titular o el participante debe ponerse en contacto con su banco central responsable para una suspensión o revocación urgente de la autorización de acceso a TARGET2 en el componente IAM (Identity and Access Management) Los bancos centrales nacionales normalmente tienen un horario de atención desde las 6:30 hasta las 18:45 todos los días laborables en TARGET2; en cualquier caso, el participante deberá comprobar con su banco central el horario disponible. El banco central informará inmediatamente a la "SSP Service Desk", quien procederá a suspender o revocar el correspondiente usuario en la IAM en ese momento.

Después, el participante enviará el formulario de solicitud para la suspensión o revocación del certificado a su banco central responsable de acuerdo con los procedimientos establecidos a nivel nacional.

Una vez que el banco central nacional recibe el formulario, comprobará su autenticidad y lo hará seguir a la "SSP Service Desk" que registrará la solicitud en el sistema PKI certificado y notificará al banco central nacional la fecha y hora de suspensión o revocación efectivas.

El banco central nacional notificará al titular y al participante la suspensión o revocación del certificado, especificando la fecha y hora desde las que el certificado no es válido.

6.2 Causas de la suspensión o revocación de certificados

El titular o el participante pueden solicitar a su banco central responsable, la suspensión o revocación de un certificado por alguna de las causas listadas en la siguiente tabla.

CAUSA	**SOLICITANTE**	
	TITULAR (EMPLEADO O PERSONAL EXTERNO)	**PARTICIPANTE**
PÉRDIDA DE LA TARJETA	**X**	**X**
ROBO DE LA TARJETA	**X**	**X**
PÉRDIDA DE SEGURIDAD	**X**	**X**
DETERIORO DE LA TARJETA	**X**	**X**
CAMBIO DE PUESTO DEL TITULAR[4]	-	**X**
OTRO[5]	**X**	**X**

[4] Causa que debe indicarse, por ejemplo, cuando el titular cesa en su trabajo.
[5] Cualquier otra causa; por ejemplo, solicitud de revocación debido al cese de la actividad como resultado de una fusión, liquidación, etc.

En el caso en el que se indique como causa “otro”, deberá darse una causa adecuada.
Excepto en el caso de robo o pérdida, el titular debe devolver la tarjeta o el *token USB* al participante después de inutilizarla cortando el microcircuito.

6.3 Reactivación de certificados suspendidos

Si se solicitó la suspensión de un certificado y después se ha recuperado la tarjeta, puede solicitarse la reactivación del certificado suspendido; si, por el contrario, la pérdida se confirma, el titular debe solicitar su revocación.
Con la solicitud de reactivación se seguirá el mismo procedimiento que con la solicitud de la suspensión.
La Autoridad de Certificación reactivará el certificado, eliminándolo de la Lista de Certificados Suspendidos.
La Autoridad de Certificación, a través del banco central responsable, notificará al titular de la tarjeta y al participante la reactivación del certificado, especificando el día y la hora desde las que el certificado nuevamente está activo.

6.4 Revocación de los certificados por decisión de la Autoridad de Certificación

En siguientes casos excepcionales, la Autoridad de Certificación revocará los certificados para el par de claves guardadas en sus bases de datos internas:

1 en el caso de pérdida de seguridad de la clave privada, por ejemplo, si se compromete la fiabilidad de sus medidas de seguridad,

2 cese de la actividad.

La revocación se llevará a cabo, incorporando los certificados a la Lista de Certificados Revocados.
Cuando la revocación se deba a la pérdida de seguridad en la clave privada de la Autoridad de Certificación, ésta actuará de forma unilateral revocando todos los certificados firmados con esa clave.

7 Procedimiento para la renovación de certificados

Las claves electrónicas son válidas durante **3 años**.

Cuando se aproxime la fecha de expiración de los certificados, la “SSP Service Desk” enviará una notificación a los bancos centrales con la lista de personas de cada participante cuyos certificados van a expirar en los próximos dos meses. El banco central comunicará esta información a los participantes afectados siguiendo los procedimientos establecidos a nivel nacional.
Antes de la fecha de expiración del certificado, su titular podrá renovarlo accediendo a la página web que pone a disposición la Autoridad de Certificación para generar un nuevo par de claves. En este caso, no hay que realizar ninguna acción adicional. Por tanto, es muy recomendable ejecutar la renovación a través de este procedimiento, antes de llegar

a la fecha de expiración. Esto asegura que no hay cortes en la validez del certificado y en la capacidad para operar.

Si la solicitud de renovación de los certificados se realiza después de su fecha de expiración, el participante deberá solicitar a su banco central responsable, la emisión de unos certificados idénticos a los expirados a través de un formulario específico, siguiendo los procedimientos que defina cada banco central. El banco central nacional enviará el formulario a la "SSP Service Desk" que hará llegar al banco central los sobres con los códigos de acceso a la aplicación web a través de la que podrá descargar los nuevos certificados. Para la entrega y recepción de estos códigos, se aplicarán las reglas establecidas en el punto 4.3 para la entrega de los dispositivos de seguridad.

Anejo 1. Lista de Formularios

1. C100 - Application for issue of electronic certificates
2. C110 - Information note on personal data protection
3. C120 - Request for suspension of electronic certificates
4. C125 - Request for reactivation of suspended electronic certificates
5. C130 - Request for revocation of electronic certificates
6. C135 - Request for renewal of electronic certificates

Anejo 2. Procedimiento para la obtención de un certificado electrónico

El participante directo que accede a TARGET2-Banco de España a través de Internet deberá solicitar la emisión de los certificados necesarios para identificar a los usuarios que operarán en el ICM. Para ello, remitirá firmado el formulario **C100** por cada certificado que necesite. El titular del certificado firmará el formulario C100 junto con la nota informativa recogida en el formulario **C110** que le proporcionará el Banco de España.

El Banco de España se pondrá en contacto con la SSP y la Autoridad Certificadora para registrar los usuarios de la entidad y la emisión de los nuevos certificados. Una vez que Banco de España reciba las tarjetas que contienen los certificados y las claves asociadas, las enviará a la entidad de crédito.

El participante informará al Banco de España de que el certificado ha sido entregado a su titular y éste lo notificará a la SSP para que el certificado sea activado.

